UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/949,525	10/14/97	WIENER	M ENT970827-1

EXAMINER	
MEISLAHN,D	
ART UNIT	PAPER NUMBER
2132	17

DATE MAILED: 12/01/00

TM02/1201

CHRISTOPHER J REDMAMP
P O BOX 677
NORTH BROOK IL 60065

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.	Applicant(s)
08/949,525	Michael J. Wiener And Josanne M. Otway
Examiner	**Group Art Unit**
Douglas Meislahn	2132

☒ Responsive to communication(s) filed on *Sep 11, 2000*

☒ This action is **FINAL.**

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire *3* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claim

☒ Claim(s) *1-26* is/are pending in the applicat

Of the above, claim(s) _____ is/are withdrawn from consideration

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) *1-26* is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☒ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☐ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

DETAILED ACTION

Response to Amendment

1. This action is in response to the letter filed 11 September 2000.

Response to Arguments

2. Applicant's arguments filed 11 September 2000 have been fully considered but they are not persuasive.

3. Applicant states that the claim language proposes a system in which a user cannot select the expiry time of a public/private key pair. This assertion is incorrect. At no point does the claim language support this conclusion. Incidentally, applicant states in the sixth line of the second full paragraph on page 2 of the response that they "claim a multi-client trust authority . . .." There is no multi-client trust authority recited in the claims, nor can this entity be found in the specification. With respect to applicant's complaints about the application of Ellison to claim 1, the claim does not touch on the origin of new keys, and Lewis is present to lay groundwork for Ellison's system. Applicant's arguments with respect to claims 2, 6, and 9 are similarly deficient.

4. In response to applicant's argument that Lewis is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, both Lewis and Ellison are concerned with public key cryptosystems.

5. Initiating the update of keys by an e-mail message is a type of update privilege control, which explains the rejection of claim 3. With respect to claim 4, Ellison's discussion on page 3 of a key, the existence of which need not be known to a CA, meets the limitation of sending keys from a user to a CA. The other limitations of this claim are obvious in light of that teaching. Claim 8 can be interpreted as adding no new material and hence need not be treated. Most of the limitations of claim 10 are inherent; storing the digital signature key pair and associating data that is supposed to be associated must be done for the process to work. The other limitation is met by the discussion of claim 4. Claims 11 is similar to claim 2, especially considering that encryption certificates and digital signature certificates can be the same. Claim 12 is similar to claim 3. Ellison has been used to show the benefits of selectable expiry data of digital signature keys, which include private keys and thus reads on claim 13. Claim 14 is a system for method claim 1. Claims 15 and 16 have the same features as claims 2 and 3. Claim 17 is means for performing claim 16. Claim 18 is means for performing claim 4. Claim 20 and 26 are similar to claim 6, while 24 corresponds to claim 4.

6. In response to applicant's arguments against the references individually with respect to claims 5, 7, 19, and 25, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-4, 6, 8-18, 20-24, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (5761306) in view of Ellison (Generalized Certificates).

Lewis shows a public key replacement system. Figure 2 shows that both private and public keys are updated. Lewis' system causes a key switch. Lewis does not say that there are certificates with expiry data that is user selectable. Ellison talks throughout his disclosure about certificates, which are used to authenticate public keys. These certificates are issued by certification authorities. On page five, Ellison says that he believes that there is a problem with CRLs. He believes, as he says in the paragraph bridging pages five and six, certificates should each include a validity field. He goes on to say that "[i]t is up to you to decide how long you're willing to have an invalid certificate out in the world – and to define the validity period accordingly. This is a matter of normal risk management." An example of decisions made based on risk management is demonstrated by buyers of RSA's keys; users can get a short-lived key pair for free but have to pay for longer lasting keys. An e-mail message that begins on page seven and ends on page 9 of Ellison's article outlines the benefits of eliminating CRLs. Therefore it would have been obvious to a person of ordinary skill in the art at

the time the invention was made to give users the ability to define the validity period for certificates, as taught by Ellison, in the public key update system of Lewis.

Additional material in claim 9 is anticipated by Lewis. Claim 2 is shown by Ellison. Claim 3 is met by Lewis in lines 64-65 of column 7. Claim 6 is inherent to Ellison in that an interface to select validity periods is required.

9. Claims 5, 19, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis and Ellison as applied to claims 1, 14, and 21 above, and further in view of applicant's admitted prior art.

Lewis and Ellison teach the selection of key validity periods on a per client basis. They do not specify a time frame in which a client can request key updates. In lines 14 through 19 of page 2, applicant discusses a conventional public key system in which keys have a fixed default period that is " . . . generally a fixed percentage or a total key lifetime . . .." Official notice is taken that fixed length renewal periods are old and well-known. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to set key update periods that are based on a fixed number of days and a percentage of a key's lifetime. This method provides flexibility by giving clients who have keys that have either extremely long or extremely short lifetimes two options as to when to update their keys.

10. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis and Ellison as applied to claim 1 above.

Lewis and Ellison teach the selection of key validity periods on a per client basis. In their system, keys are created by a user and then sent to a certification authority for a

certificate. In another implementation of public-key cryptosystems, the certification authority both generates and verifies the public/private key pair, sometimes on request. The previously mentioned RSA key marketing method exemplifies this. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to apply the teachings of Lewis and particularly Ellison to the well-known public key cryptosystem where a certification authority produces the key pair.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached between 9AM - 6PM, except for every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann can be reached on (703) 308-7791. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 308-9051 for regular communications and (703) 308-9052 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J. Meislahn
Examiner
Art Unit 2787 2132

DJM
November 30, 2000

TOD SWANN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100